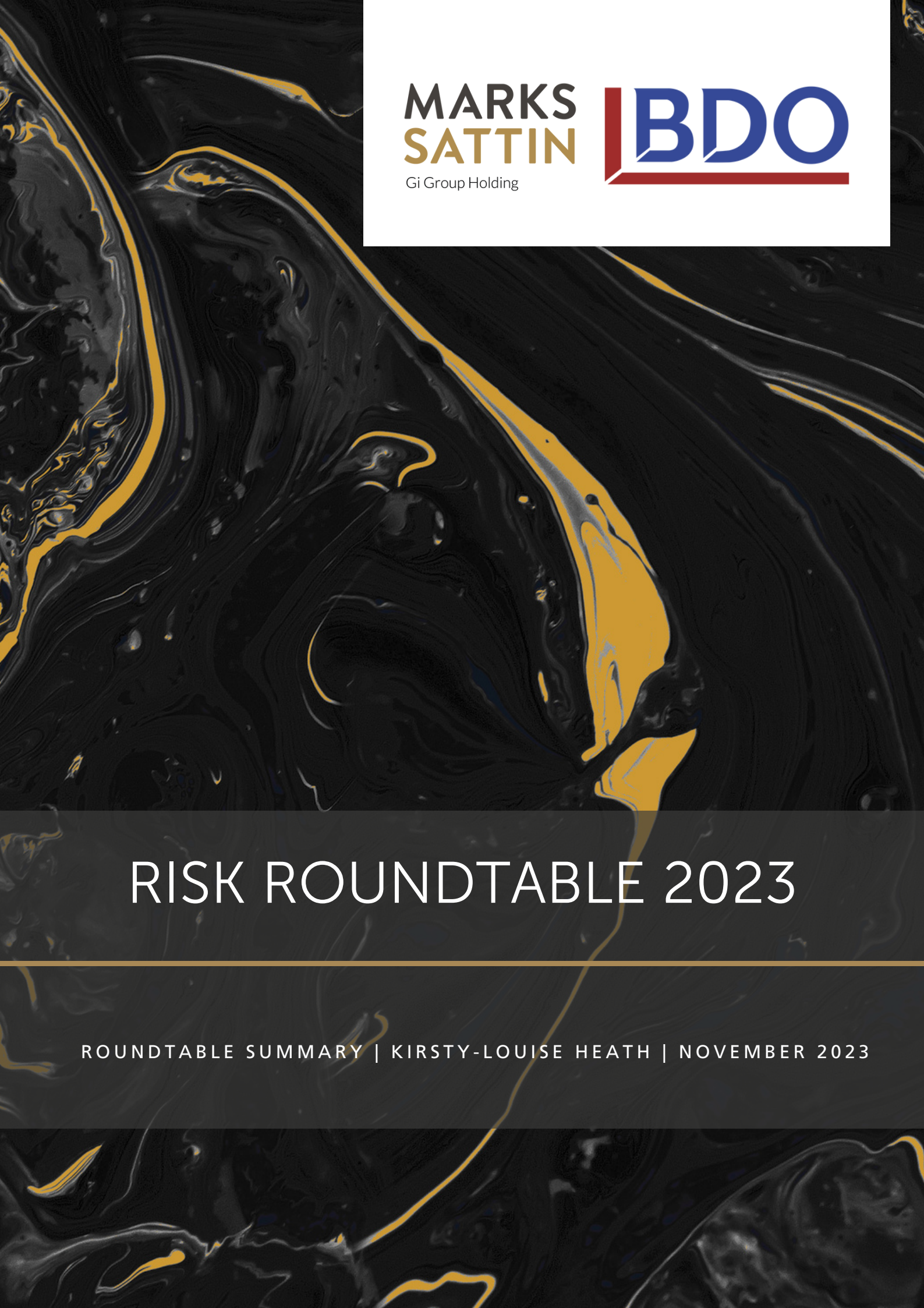


RISK ROUNDTABLE 2023

ROUNDTABLE SUMMARY | KIRSTY-LOUISE HEATH | NOVEMBER 2023

OVERVIEW

Marks Sattin, in conjunction with BDO, ran a Risk Roundtable event in Leeds to exchange useful ideas, insights and experiences on key topics currently facing the risk profession.

Participants were representatives from the risk community, primarily from the financial services sector. This whitepaper outlines their conversation, and covers the following topics:

Processes & reporting

- RCSA processes & technologies
- KRIs

Instilling Risk Culture

- Tools & techniques
- Reporting risk events
- Business incident or event & crisis management / business continuity transition

Annual Planning & Emerging Risks

- Emerging risks identification
- Approaches
- Managing emerging risks

Industry Topics

- Consumer duty
- Operational resilience

HOT TOPICS

RISK AND CONTROL SELF-ASSESSMENT (RCSA) PROCESSES

The group outlined various approaches to RCSA experienced and, while each process had its merits and disadvantages, it was top-down rather than bottom-up that was most in use. One of the participants has only recently started using RCSA and is doing so from a bottom-up approach, but, following the meeting, that approach is being reconsidered.

The executive teams were found to prefer the top-down approach because this resulted in risks reported at a level that was more relevant to them. Conversely, a bottom-up approach tends to see greater engagement from First Line of Defence (1LOD) because of the nature of the level of granularity involved with which they are more comfortable.

Instances were discussed where the Financial Conduct Authority (FCA) participated in the RCSA process. They recommend conducting this at the process level, and it was noted that where they are involved, there is a greater up take u and success.

Furthermore, greater success also results when ownership and responsibility are clearly defined and are accepted. Often, workshops are held between the risk team and either 1LOD or the executive team once the initial RCSA has been issued. Here, the RCSA responses are collated and discussed, facilitated by the Risk team. It was recognised that whilst this was a time invasive exercise, it is a valuable investment because of the increased risk awareness resulting from it. The challenge following this is the extent to which that awareness is maintained, and the continued actions to sustain effective risk management. This boils down to continued education, which was found to be an ongoing exercise.

Concerns were also raised that RCSA sometimes becomes a tick box exercise, thereby diminishing its inherent value. This can be despite the education exercises conducted. The importance of risk management are its benefits to the organisation and need to be reiterated in these instances.

It was also noted that there is greater success in RCSA when the basis for the risk classification is clearly understood (e.g. why a risk classified is classified in the way it has been), the rationale for the control to mitigate the risk is defined and communicated (demonstrating that it is the right control), and the description of that control is clear and unambiguous. Where these are lacking, a loss of confidence in the process results.

RCSA TECHNOLOGIES

Various tools1 used were discussed, each with varying degrees of success. It was noted that it is important to consider and clarify their intended use, the deliverables required, and the level of support offered by the vendor.

SIMON, for example, was noted as particularly good but had limitations over its reporting. Riskonnect was mentioned by several participants, one of whom is currently investigating its functionality. Whilst it was praised, it was not particularly flexible to meet all requirements, and did not include the fundamental ability to specify the risk appetite.

KEY RISK INDICATORS (KRIS)

THE GROUP ADMITTED THAT KRIS POSE A NUMBER OF CHALLENGES. THESE INCLUDED:

- Defining the KRI itself. Limitations in identification and specification can lead to inaccurate alerts being produced
- Obtaining the right data to be used as a KRI
- Timeliness of reporting to ensure that the risk can be managed effectively
- The organisation's culture

MARKS SATTIN
Gi Group Holding

The key takeaway was that KRIs should not be seen in isolation.

A measured approach that considers the risk appetite, culture, strategic objectives, and current commercial factors results in a more practical management of risk, and at the same time can help improve the perception of Risk function within the organisation.

Trend analysis for KRIs was the most used amongst the group but this still has challenges, such as timeliness of reporting.

KRIs can be out of date very quickly and so it is important to regularly review the metrics to ensure they remain relevant. Instances were mentioned where the KRI had been amber or even red for some time and management had subsequently become de-sanitised from it.

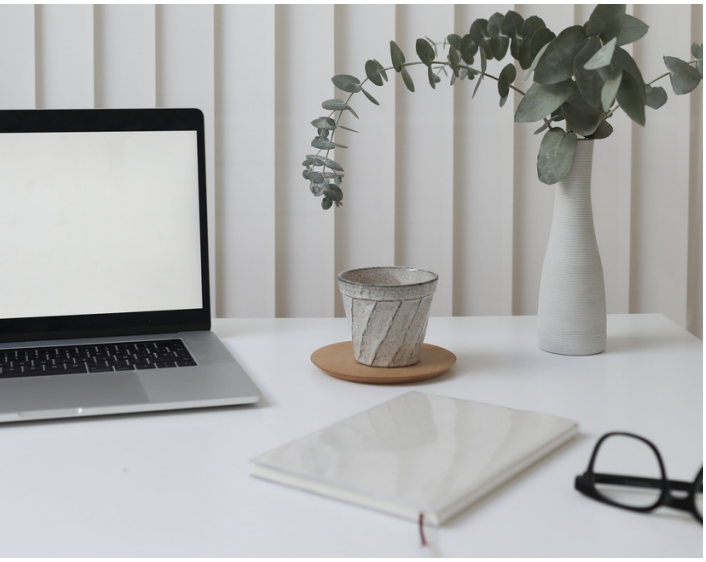
Regulators are often seen as facilitators in ensuring that these are regularly reviewed, especially if the business priorities do not allow this to be completed in a timely manner.

It was noted that identifying the cause of the risk to materialise often helps in developing the indicator. An example of problems at the house building stage was muted as an indicator for a downturn in the economy.

The risk appetite should also be considered when assessing the KRIs, both in terms of specifying the KRI in the first place, but also in reviewing the indicator's output in reviewing the risk.

It was noted that there is value in learning from the risks that have materialised, where the risk appetite has been breached, providing these learnings can be operationalised, not just recorded.

One participant found it beneficial to adopt a forward-looking approach that considers the potential impact of measures currently undertaken in the business, such as the introduction of a new product, to facilitate the identification of risks downstream.



Indicators may point to wider issues, such as complaints leading to mis selling, or the inadequacies in a process, such as the number of 'drop-outs' in an application mechanism that may indicate something wrong with the process, not the actual quality of the application for a product.

The culture of the organisation can have a significant impact on the attitude towards risk and therefore KRIs. Senior management often see the Risk community as negative and as potential 'blockers' to the achievement of strategic objectives. But a greater understanding of risk helps embed KRIs, in line with the organisation's risk appetite. Further, a negative perception of the Risk function can be reversed when risks are repackaged as aiding the organisation to achieve its strategic objectives.

It was noted that a subjective impression of risks within the market can compare favourably to quantifiable KRIs. This reinforces the point that KRIs should not be relied upon in isolation, but be assessed in the context of other aspects, such as the organisation's risk appetite and its culture.

INSTILLING RISK CULTURE

Discussions on risk culture inevitably focussed on the role of senior management and whether they were supportive. Tone from the top was seen as the most effective way to embed a risk culture within an organisation. This too has challenges, however, especially when the executive team do not fully understand risk management.

Some organisations needed to spend a lot of time with the executive and senior management team to assist them in improving risk awareness and processes. Sometimes, this meant going back to basics, helping them understand, for example, what a risk is, or what risk appetite means. This has been most effective through interactive workshop sessions. The key challenge is to maintain that interest and energy.

Some senior teams, however, have been reticent because weaknesses in the risk and control environment may be perceived as a failure of their own performance. The challenge therefore is how to turn this on its head so that any identified weaknesses are seen as an opportunity to strengthen the control environment, not as criticism of senior management.

It was noted that there are pockets in some teams across organisations that are more engaged in risk processes than others.

ONE PARTICIPANT NOTED THAT IT IS IMPORTANT TO REMIND THOSE IN 1LOD THAT IF THEY ARE RESPONSIBLE FOR AN AREA OF THE BUSINESS THEY ARE RESPONSIBLE FOR RISK AND TO REMEMBER THE MANTRA, "EVERYONE IS A RISK MANAGER"

This is not always grasped or agreed with. In some instances, the Risk team make recommendations to management on how to improve the management of the risk, and the business, with clear responsibility over that risk, needs to explain to the Risk Committee if this is not being met. This is particularly effective where there is support for the approach from the executive team. One organisation reported having risk representatives embedded within 1LOD, with the result that 2LOD is relatively 'thin'.

The onus for risk is therefore pushed to 1LOD to own and manage the risk. Its effectiveness may depend on the quality and extent of training provided. Regular training, from induction onwards, was seen by all as the most beneficial way to instil risk awareness, in conjunction with regular support from the risk team.

There are always some cultural or personal limitations, where responsibility and accountability are unclear or if the individual just does not fully understand or even agree that risk is part of their responsibilities.

A key aspect of risk was noted as psychology. The negative perception of the Risk team can and should be turned on its head to demonstrate how risk management can help an organisation achieve its objectives. This can be assisted by calling out when the identification and management of risk through effective controls has resulted in a positive outcome.

It is important, given the pace of change in today's markets, that the risk appetite should be regularly reviewed to ensure it continues to reflect the organisation's attitude to risk and so is best able to achieve strategic objectives.

It was noted that Financial Services organisations are more familiar and comfortable with the concept of formal risk management than other sectors, so the challenge is to instil risk management in all industries without it being, perceived or actual, an unnecessary overhead.

It was pointed out that a whistleblowing culture may be seen as positive, but that might not be the case.

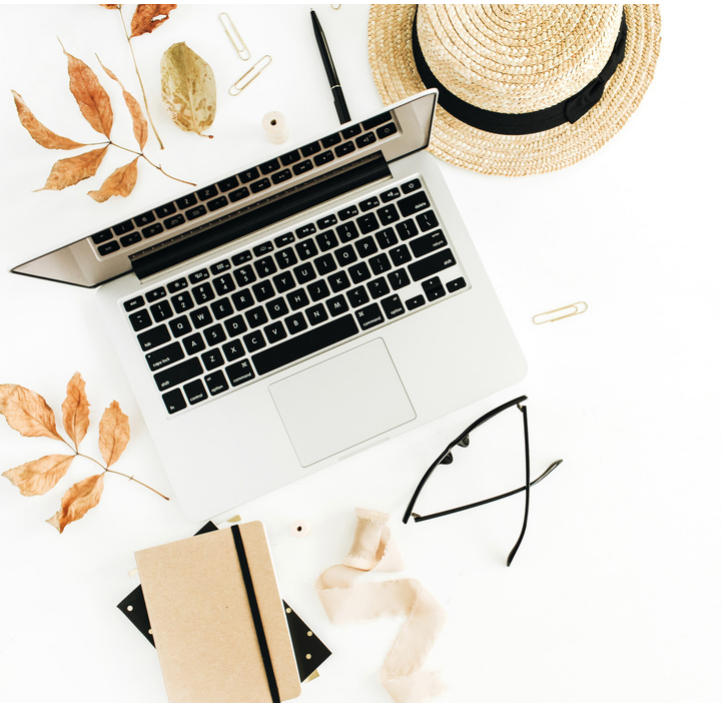
IT MAY MEAN THAT THE CULTURE OF THE ORGANISATION DOES NOT LEND ITSELF TO WHISTLEBLOWING, WHICH HAS A DETRIMENTAL EFFECT ON THE OVERALL RISK MANAGEMENT MECHANISM. IN SUCH INSTANCES, THE MINDSET NEEDS TO ENSURE THAT REPORTING INCIDENTS IS SEEN AS POSITIVE. THIS IS FURTHER ENHANCED NOT ONLY BY ACTIONS BEING TAKEN BECAUSE OF THE REPORT (WHERE APPROPRIATE) BUT ALSO BY BEING SEEN TO BE TAKEN, WHICH IN TURN PROMOTES EMPLOYEE ENGAGEMENT.

REPORTING RISK EVENTS

Reporting risk events accurately and promptly is most effectively achieved when colleagues understand what a risk is and what their responsibilities are towards risk, including reporting, especially where these responsibilities cross over several functions. This is best achieved through regular training, and often starts at induction but should be supplemented by formal training sessions.

One of the key challenges faced was the number of systems in place to record risk events. Too often, the same risk details are entered into multiple systems, making it time-consuming and laborious. The ultimate impact is that some risks may not be reported, and by its nature, it is of course not possible to determine the extent of this.

All agreed that it would be much more beneficial if the process were as simple as possible and made through one system. This should then be able to report on the various aspects of the risk given the information input, such as customer detriment or breach of regulation.



BUSINESS INCIDENT/CRISIS MANAGEMENT/BUSINESS CONTINUITY

Discussions over the definition of the point of transition between a business incident or event into crisis management/business continuity showed that this is a challenge to most organisations.

Even though there are criteria which can be applied for each that are designed to provide clarity, this was not always fully effective because there is often a level of subjectivity involved, or it has not been sufficiently defined. For example, one instance was discussed where exceptional weather did not invoke a crisis event and a severe weather plan, but a risk event was raised instead, with instructions issued to Work from Home. This was seen as a potential 'translation' point, which promotes the need for greater clarification of definitions and criteria.

Similarly, there is a challenge over how to convince senior management to make the decision as to when to invoke crisis management. An example was given where a third party had been employed for Crisis Management, but they did not adequately define when the plan should be invoked.

AUDIT PLANNING AND EMERGING RISKS

It was agreed that annual planning requires some fluidity to the process to be able to react to changes to risks, yet within a manageable framework.

It was suggested that risk assessments should be conducted more frequently to ensure that the organisation continues to focus promptly on the most significant risks and thereby remain relevant.

It is important to revisit the risks to ask whether they have changed, and should it be reprioritised within the context of other risks facing the organisation.

Some risks, such as the threat of new entrants into the Financial Services market, and the speed in which they can operate (Apple and Amazon were given as examples), has been included in emerging risks for some time but nothing yet has materialised. Furthermore, a change in mindset was said to be needed, from Black Swan2 to Grey Rhino3, with the example given of the Covid pandemic.

These examples reiterate the need to continue to be vigilant about the nature and severity of risks, and to regularly assess them. It was noted that the management of risks associated with climate change were not always included in the emerging risks register.

Discussions then expanded into risks in related aspects such as disease and biodiversity that come about due to the impact of climate change.

This developed onto risks that may not be initially apparent but may lead on to other risks downstream not previously considered. This was noted as not always considered as part of the risk planning process.

Clients are thinking increasingly about the impact of AI4 on businesses and the risk it poses, as well as using AI within risk functions to improve efficiency. As pressures grow on businesses from the increased volume of work (often set against the challenge of reducing staff numbers) and the amount of data to be processed, this can be an opportunity to utilise AI to complete more routine work and to help analyse data to obtain meaningful KPIs and KRIs for subsequent investigation. Examples were given in the use of AI to summarise large volumes of information, to produce policies or job descriptions.

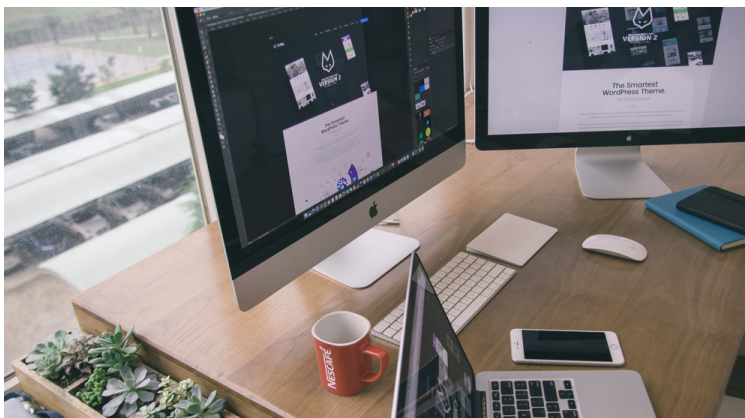
ANOTHER EXAMPLE WAS PROVIDED WHERE A BOT WAS USED TO ATTEND MEETINGS ON SOMEONE'S BEHALF, BUT THIS HAD AN IMPACT ON GDPR5 AND COMMERCIAL SENSITIVITY THAT HAD NOT PREVIOUSLY BEEN CONSIDERED.

It was noted that it is important to remember that using AI to analyse data or create output does not abdicate an individual's responsibilities over this output. It should first be reviewed before any further action is taken to ensure it is complete, accurate, timely and meets both internal and external requirements.

By extension, the risk of the organisation not understanding the algorithms that underpin the business is significant, common, and should be managed accordingly.

The risks associated with increasing inequality in the context of the cost-of-living crisis, thereby affecting both an organisation's staff and customers, was discussed. The question was raised whether this should be classed as an emerging or a current risk. This is currently manifesting itself through increased instances of theft, both by individuals and by organised gangs. This also extends further to the risks relating to the effect on individual's medical conditions and longevity through the impact on increased medical costs and pensions.

The PRA recently issued a consultation paper concerning Diversity and Inclusion (D&I). Whilst this was not seen by the group as ground breaking, it demonstrated that the regulators are now extending their traditional reach and means that organisations need to be more aware of these types of issues and the risks associated with them A key point raised was that AI should not be classed as an emerging risk because it is already here and should therefore be treated as such.



CONSUMER DUTY

The key challenge with Consumer Duty (CD) is the shift from it being a unique entity to being part of a wider piece. This brings in the questions of the responsibilities over CD and the adequacy of their knowledge and experience to ensure that CD is considered and embedded throughout the organisation.

One participant described using a professional firm to assess their CD arrangements. Whilst this raised a number of points to consider, these needed to be assessed to understand which were sufficiently significant to be addressed, and those that were more advisory given the organisation's priorities. This is a common requirement following any scrutiny by an external body to assess the organisation's capabilities over a specific area of expertise.

Another participant did not have formal compliance mechanism until recently and so this requirement is new to them. It is therefore important to consider the nature of the business in relation to the requirements of CD and how they can best meet them.

OPERATIONAL RESILIENCE

One participant raised the point that as the FCA requirement for Operational Resilience is positioned from the point of view of the customer, further work is needed to consider other elements that are not customer focussed.

The best software solution for Operational Resilience that one of the participants had seen was PROTECHT.

The conversation moved from Operational Resilience per se to the risks associated specifically with Cyber Security. It was noted that the Bank of England expects each Financial Services organisation to have cyber security in their top three risks. Cyber security programmes were said to be ongoing, because of its fast-moving nature and regular new challenges. This relentless number of programmes to raise awareness can have the opposite than intended affect because colleagues may become immune or complacent to these threats. Ironically, there have been examples of greater number of successful cyber-attacks.

Conversely, there have been instances of increased incident reporting because of the training, due to colleagues seeing everything as significant that should be reported. This reiterates the need to understand the threats and to maintain vigilance over the risks facing organisations against the challenge of the plethora of training programmes in place.

There was not time to talk through all the topics outlined today, but it is hoped that these will be covered in future sessions:

- Supplier Management
- Risk Coalition
- Mortgage Charte

If you have any feedback or would like to discuss your recruitment needs, please contact me:

Kirsty-Louise Heath
Senior Consultant
kirsty.heath@markssattin.com